

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of: <i>Dunkeld et al</i>) Art Unit: 3621
)
Serial No.: 10/016,325) Examiner: <i>Augustin, Evens J</i>
)
Filed: 12/10/2001)
)
For: <i>System & Method for Unique Digital Asset</i>)
<i>Identification and Transaction Management</i>)

Appeal Brief filed under 37 C.F.R. § 1.192

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

Per 37 C.F.R. § 41.37 Appellants submit the present Appeal Brief in furtherance of the Notice of Appeal filed in this case on October 7 2010. Please charge any fees, including for an extension of time, in accordance with the accompanying Transmittal letter. This brief contains the following sections as required by 37 C.F.R. § 41.37 and MPEP § 1206:

- I. Real Party In Interest
- II. Related Appeals and Interferences
- III. Status of Claims
- IV. Status of Amendments
- V. Summary of Claimed Subject Matter
- VI. Grounds of Rejection to be Reviewed on Appeal
- VII. Argument
- VIII. Claims
- IX. Evidence
- X. Related Proceedings
- Appendix A Claims

I. REAL PARTY IN INTEREST

Kopesh LLC, dba Meridian Ventures an LLC having a place of business at 3011 68th Avenue SE, Mercer Island, WA 98040.

II. RELATED APPEALS AND INTERFERENCES

None.

III. STATUS OF CLAIMS

Claims 22 – 37, 55 and 59 - 83 are rejected and the subject of the present appeal. All other claims are withdrawn or canceled. A complete copy of the claims and their status is provided in Appendix A.

IV. STATUS OF AMENDMENTS

There are no non-entered amendments.

V. SUMMARY OF CLAIMED SUBJECT MATTER

Independent claim 22

i. Independent claim 22 covers:¹

A system for exchanging digital assets over a network, comprising: (*FIG. 1; page 15, l.6 – page 17, l. 7*)

(a) a first computer coupled to the network, said first computer storing a digital asset which includes both digital content and a first unique identifier associated with a first instantiation of said digital asset; and (*see FIG. 1, box 106 and specifically box 116; pages 18, ll.20+*)

(b) said first computer being adapted to set up a customer account and an authorization to play said digital asset on a second computer coupled to the network; and (*id. boxes 112 and 126; page 20, ll. 10+*)

(c) a first software routine executing on said first computer and/or said second computer, said first software routine being adapted to coordinate transfer of said digital asset to said second computer; (*FIG. 1, box 112; FIG. 2, boxes 312 – 328*)

wherein a second instantiation of said digital asset is created for said transfer to said second computer, said second instantiation including a second unique identifier including customer information associated with a customer for said digital asset; (*FIG. 1, boxes 118 – 120; FIG. 2, box 318; page 21, ll. 12+*)

further wherein said digital asset has no copy protection and can be transferred from said second computer to a third computer by said customer without requiring an additional authorization from said first computer (*page 4, ll. 15 – 18; page 5, ll. 15 – 16; page 30, ll. 16 – 18; Abstract, ll. 11+*)

¹ In the interest of efficiency and clarity Applicant has not identified every single aspect of the disclosure which may pertain to the claimed limitations.

ii. Independent claim 55

Independent claim 55 covers a method of exchanging digital assets over a network, comprising the steps of: (*FIG. 1; page 15, l.6 – page 17, l. 7*)

(a) storing a digital asset on a first computer coupled to the network, which digital asset includes both digital content and a first unique identifier associated with a first instantiation of said digital asset; and (*see FIG. 1, box 106 and specifically box 116; pages 18, ll.20+; also box 108*)

(b) setting up a customer account with said first computer including an authorization to play said digital asset on a second computer coupled to said first computer over the network; and (*id. boxes 112 and 126; page 20, ll. 10+*)

(c) creating a second instantiation of said digital asset, including a second unique identifier; (*FIG. 1, boxes 118 – 120; FIG. 2, box 318; page 21, ll. 12+*)

wherein said second unique identifier includes customer information associated with a customer for said digital asset; (*id.*)

(d) storing said second instantiation of said digital asset at said second computer; (*id.*)

wherein said digital asset has no copy protection and can be transferred from said second computer to a third computer by said customer without requiring an additional authorization from said first computer. (*page 4, ll. 15 – 18; page 5, ll. 15 – 16; page 30, ll. 16 – 18; Abstract, ll. 11+*)

iii. **Independent claim 75**

Independent claim 75 covers a method of exchanging digital assets over a network, comprising the steps of: (*FIG. 1; page 15, l.6 – page 17, l. 7*)

- (a) providing a first computing system coupled to the network; (*see FIG. 1, box 108*)
 - (b) storing a digital asset in one or more storage systems accessible to said first computing system, which digital asset includes both digital content and a first unique identifier associated with a first instantiation of said digital asset; and (*see FIG. 1, box 108/122*)
 - (c) providing a second computing system which is coupled to the network and implements a digital asset management system which stores transaction information concerning said digital asset; (*see FIG. 1, box 106 and specifically box 116; pages 18, ll.20+; also box 108*)
 - (d) selectively coupling said first computing system to a third computing system in response to a request made for said digital asset by a routine executing on behalf of said third computing system; and (*id. boxes 112 and 126; page 20, ll. 10+*)
 - (e) processing said request at said second computing system to generate an authorization for a transfer of said digital content of said digital asset; (*id. boxes 112 and 126; page 20, ll. 10+*)
 - (f) determining which one or more of said one or more storage systems should be used to transfer said digital content for said digital asset; (*id.*)
 - (g) creating a second instantiation of said digital asset for said request, including a second unique identifier; wherein said second unique identifier includes customer information associated with a customer for said digital asset; (*FIG. 1, boxes 118 – 120; FIG. 2, box 318; page 21, ll. 12+*)
 - (h) transferring said second instantiation of said digital asset, including said second unique identifier, to said third computing system from one or more of said one or more storage systems based on said authorization; (*FIG. 1, box 112; FIG. 2, boxes 312 – 328*)
- updating said transaction information at said second computing system based on said transfer; (*id.*)

wherein each transfer of said digital asset between different computing systems is associated with a unique identifier embedded within the digital asset to facilitate tracking across the network, such that different versions of the digital asset are created for said transfers, and each version carries a complete transaction record of transfers of prior versions. (*id.*; page 24, ll. 5+)

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

The issues presented for appeal are whether claims 22 – 37, 55 and 59 – 83 are patentable under § 103 over the Levy reference (US Publication No. 2002/0052885) taken with Williams (Publication No. 2002/0002541)

VII. ARGUMENT

Background

The present invention relates, in general, to the field of distribution of digital asset content. The disclosure posits systems and methods which, unlike prior art systems which rely solely on encryption or other encumbrances such as digital rights management (DRM) overhead, instead allows assets to be freely transferred without copy protection between the customer's devices. The main overhead imposed by the system instead is in the use of tracking of assets, which can be done easily and without significant burden on the users of the system after they set up an account and are authorized to play the assets. The claimed system here creates a new version of the asset for each transfer, including a unique identifier which includes some customer information. While other conventional forms of encryption, steganography, etc., can be used with the disclosed embodiments, the key feature of the claimed methods is in the use of unique identifiers and lack of copy protection overhead which allows for easy tracking of the assets throughout a network of client systems.

Claims 22 – 37, 55 and 59 - 83 are Patentable Over Levy and Williams

The Examiner's rejection is based on Levy and Williams to argue that the claims would have been obvious. This argument is not supportable however as references do not actually collectively teach the limitations of the claims, and, moreover, there is no teaching or suggestion for the Examiner's proposed combination.

To wit, Applicant has pointed out (on several occasions now) that the Office Action fails to make a prima facie case against the claims because the Examiner has not addressed several limitations. As there is no evidence presented in the record to date against these limitations, Applicant submits that the rejection must be reversed.

The References Do Not Teach At Least Two Key Limitations – Including “...a second instantiation” that has “a second unique identifier including customer information” and that the digital asset has “...no copy protection....”

“[T]he examiner bears the initial burden, on review of the prior art or on any other ground, of presenting a prima facie case of unpatentability.” In re Oetiker, 977 F.2d 1443, 1445 (Fed. Cir. 1992). In rejecting claims under 35 U.S.C. § 103, it is incumbent upon the Examiner to establish a factual basis to support the legal conclusion of obviousness. See In re Fine, 837 F.2d 1071, 1073 (Fed. Cir. 1988). The Examiner’s articulated reasoning in the rejection must possess a rational underpinning to support the legal conclusion of obviousness. In re Kahn, 441 F.3d 977, 988 (Fed. Cir. 2006).

The rejection of claim 22 fails for, among other reasons, the fact that neither Levy nor Williams is ever argued or shown by the Examiner to have:

“.. a second instantiation of said digital asset is created for said transfer to said second computer, said second instantiation including a second unique identifier including customer information associated with a customer for said digital asset;”

The Board will note that, while the Office Action purports to address many limitations in claim 22, there is nothing in paragraphs 4(A) to 4(R) which discusses this type of second instantiation of the digital asset. The closest the Examiner comes to an actual discussion is in paragraph 4(P), but that discusses a certain type of “second instantiation”...” created in accordance with distribution rules” and is apparently directed to claim 73, not claim 22. Thus, as a matter of law, the rejection cannot be sustained because the Examiner has failed to specifically articulate and point out anything in the reference that meets this limitation. This is precisely the type of broad brush rejection which was repudiated in Ex parte Blanc, 13 USPQ 2d 1383, 1384 – 85 (B.P.A.I. 1989).

From a review of the Office Action Applicant speculates, but cannot be certain, that the Examiner’s evidence on this point is in paragraph 4 (R). However, this passage

is directed to a discussion of Williams, and specifically that portion of the reference which the Examiner contends shows that content can be *encrypted* using a “unique identifier.” Since the Examiner does not equate anything in the discussion in Williams with a “second instantiation” of a digital asset as set out in claim 22 which *includes* the second unique identifier as part of the asset – as opposed to an asset *encrypted using* a unique identifier as purportedly shown in Williams – Applicant submits that the evidence is again unavailing because it is vague and requires one skilled in the art to speculate on how such teaching would result in the claimed limitation.

The cases are clear that it is improper to resort to speculation or unfounded assumptions to supply deficiencies in the factual basis for a rejection. See In re Warner, 379 F.2d 1011, 1017 (CCPA 1967) (“[The Patent Office] may not, because it may doubt that the invention is patentable, resort to speculation, unfounded assumptions or hindsight reconstruction to supply deficiencies in its factual basis.”). Yet that is exactly what is occurring here and which should be rejected.

More fatal to the present rejection is the fact that the Examiner acknowledges that Williams specifically uses the identifier as a form of copy protection for the digital asset. See e.g., Office Action (emphasis added):

Therefore, it would have been obvious for one of ordinary skill in the art at the time of applicant's invention to construct a unique identifier as described in Williams to modify Levy's invention. According to Williams, the motivation to use such a unique identifier would be to prevent reverse engineering of the identifier, which could allow for unauthorized duplication of content received.

Given this explanation of the teachings of Williams, and the motivation for combining with Levy, the Honorable Board must conclude that it teaches away from the claimed invention, which specifically recites that there is no copy protection. That is, the Examiner indicates that William's unique identifier would prevent reverse engineering of the identifier, and act to prevent unauthorized duplication (copying) of the content. The

problem with this logic is that William's identifier, as the Examiner acknowledges, is a form of copy protection; that is, it is used directly as a key to encrypt the content to prevent copying. This is in direct contravention to the claim language which states:

....further wherein said digital asset has no copy protection

Applicant submits that there is no possible interpretation of this limitation (let alone a "reasonable" interpretation") that could be met by a system like Levy/Williams which in fact is using a form of copy protection as the Examiner notes. Williams further emphasizes this aspect of its operation:

....distribution module 316 (or another appropriate module) suitably encrypts the content to prevent unauthorized copying/redistribution..." See paragraph 47.

Accordingly Williams cannot possibly meet this limitation of the claim.

Nor would one skilled in the art "add" Williams to Levy to add this type of encryption, since the latter already includes a detailed discussion of copy protection techniques. In fact Levy specifically mentions that the "...embedded data includes a copy control bit..." – see paragraph 68. Thus, it doesn't matter how the Examiner "modifies" the Levy digital asset with Williams, the former will still include copy protection in contradistinction the language of claim 22.

Appellant submits that from an obviousness perspective, there could not be a clearer example of teaching away by the references. Reversal of the rejection is earnestly requested.

Dependent claims 23 - 37 should be allowable for at least the same reasons as claim 22. In addition, for claim 24, it can be seen that there is no evidence of a "third" instantiation mentioned anywhere in the references; paragraph 72 of Levy for example makes no mention of any such type of feature.

Independent claim 55 should be allowable for similar reasons. Dependent claims 59 - 74 should be allowable for at least the same reasons as set out above for claims 22 – 37.

Independent claim 75 is allowable for similar reasons. Moreover the Applicant amended the claim to indicate that the digital asset carries a complete transaction record of transfers of prior versions. The Examiner makes no mention anywhere of where such limitation is found anywhere in any of the prior art, and thus has not established a prima facie case against this claim. Applicant finds no such mention either.

Dependent claims 76 – 80 should be allowable for at least the same reasons. As noted before, Levy does not teach “determining a source of a prior transfer” of an unauthorized version. At best it can apparently only identify the existence of an unauthorized copy.

Claims 81 – 83 are dependent on claim 22 and merely describe narrower embodiments of the invention identified on pages 22 (ll. 14+ and 29 - 30) and page 29 (ll. 20 – 24)(time stamps); page 28 line 20 (advertisements). As with many of the claims above, the Examiner does not cite to anything in the reference which meets the limitations of these claims, and thus has not established a prima facie case.

VIII. CLAIMS

A copy of the claims involved in the present appeal is attached hereto as Appendix A.

IX. EVIDENCE

No additional evidence pursuant to §§ 1.130, 1.131 or 1.132 or entered by or relied upon by the Examiner is being submitted.

X. RELATED PROCEEDINGS

No related proceedings are referenced herein, nor are copies of decisions in related proceedings being provided, as there are none. Accordingly, no Appendix is included.

Respectfully submitted,

A handwritten signature in cursive script, appearing to read "J. Nicholas Gross".

J. Nicholas Gross
Registration No. 34,175
Attorney for Applicant(s)

January 7, 2011
Box 9489
Berkeley, CA 94709
510-540-6300/510-540-6315 (fax)

APPENDIX A

1. (Withdrawn) A system for distributing digital assets across a network, including between a first network device and a second network device, the system comprising:
 - (a) first rights-holder server coupled to the network, said first right-holder server being adapted to introduce a digital asset for distribution, said digital asset having an associated first set of distribution rules; and
 - (b) a second host server coupled to the network, said second host server being adapted to store and distribute said digital asset; and
 - (c) a third management server coupled to the network, said third management server being adapted to track transfers of said digital asset over the network and to generate tracking records associated with said transfers;
wherein said transfers over the network involving said digital asset between the first network device, the second network device and/or the second host server are processed in accordance with said first set of distribution rules.
2. (Withdrawn) The system of claim 1, wherein the first network device can obtain said digital asset from the second network device and/or said second host server, and without requiring further authorization from said first rights-holder server.
3. (Withdrawn) The system of claim 1, wherein a modification is made to said digital asset for each transfer, said modification being used by said third management server for generating said tracking records.
4. (Withdrawn) The system of claim 3, wherein said modification does not alter user-perceptible content of said digital asset.
5. (Withdrawn) The system of claim 3, wherein said modification alters and/or adds an identification label for said digital asset so that each transfer of said digital asset is associated with a unique identification label.
6. (Withdrawn) The system of claim 1, wherein said second host server is implemented by at least one of the first network device or the second network device, so that transfers of said digital asset are performed in a peer-to-peer manner across the network.
7. (Withdrawn) The system of claim 1, wherein said digital asset includes audio, video, picture and/or text based data.

8. (Withdrawn) The system of claim 1, wherein a second set of distribution rules can be introduced by said first rights-holder server to affect transfers of said digital asset over the network.
9. (Withdrawn) The system of claim 1, wherein the network includes the Internet.
10. (Withdrawn) The system of claim 1, wherein said first set of distribution rules includes indexing information, terms of use, and a location of said second host server.
11. (Withdrawn) The system of claim 1, wherein said digital asset is also encrypted and/or contains steganographically processed data so as to reduce unauthorized transfers over said network.
12. (Withdrawn) The system of claim 1, wherein a new instantiation of said digital asset is created for each transfer occurring over the network between peer devices.
13. (Withdrawn) The system of claim 1, wherein said first network device is integrated within a fixed personal entertainment system, including a gambling machine, a digital jukebox, and/or a passenger seat.

14. (Withdrawn) A system for introducing digital assets into an electronic network distribution system, comprising:

- (a) a first computer coupled to the electronic network distribution system; and
- (b) a first software routine executing on said first computer, said first software routine being configured to perform at least the following operations:
 - i) receiving and storing a digital asset on said first computer; and
 - ii) processing administration information for said digital asset, including an asset identifier and a rights-holder identifier, and associating the same with said digital asset; and
 - iii) interacting with a digital asset management system to generate a modified version of said digital asset, said modified version of said digital asset being based on said administration information and tracking history information provided by said digital asset management system;
 - iv) posting said modified version of said digital asset to a location suitable for download by said peer devices from the electronic network distribution system;

wherein said modified version of said digital asset is configured so that a tracking history can be maintained by said digital asset management system of each transfer of separate instantiations of said digital asset between peer devices coupled to the electronic network distribution.

15. (Withdrawn) The system of claim 14, wherein said administration information also includes terms of use and expiration data for said digital asset.

16. (Withdrawn) The system of claim 14, wherein said digital asset includes audio, video, picture and/or text based data.

17. (Withdrawn) The system of claim 14, wherein said first computer is a server coupled to the internet.

18. (Withdrawn) The system of claim 14, wherein said digital asset management system and/or said peer devices embed tracking information within said modified version of said digital asset during each instantiation of said digital asset.

19. (Withdrawn) The system of claim 18, wherein said tracking information includes a unique identifier for each transfer of said modified version of said digital asset within the electronic network.
20. (Withdrawn) The system of claim 14, wherein said first software routine is further configured to provide second administration information for a digital asset such that later instantiations of said digital asset within the electronic network distribution system are based on said second administration information.
21. (Withdrawn) The system of claim 14, wherein said first software routine is further configured to receive accounting information from said digital asset management system, including: (a) information concerning the number of instantiations of said digital asset created by transfers within the electronic network distribution system; (b) revenue derived from and/or to be credited for said transfers.

22. (Rejected) A system for exchanging digital assets over a network, comprising:
- (a) a first computer coupled to the network, said first computer storing a digital asset which includes both digital content and a first unique identifier associated with a first instantiation of said digital asset; and
 - (b) said first computer being adapted to set up a customer account and an authorization to play said digital asset on a second computer coupled to the network; and
 - (c) a first software routine executing on said first computer and/or said second computer, said first software routine being adapted to coordinate transfer of said digital asset to said second computer;
- wherein a second instantiation of said digital asset is created for said transfer to said second computer, said second instantiation including a second unique identifier including customer information associated with a customer for said digital asset;
- further wherein said digital asset has no copy protection and can be transferred from said second computer to a third computer by said customer without requiring an additional authorization from said first computer.
23. (Rejected) The system of claim 22, wherein said first computer and said second computer operate to transfer said digital asset in a peer to peer manner across the Internet.
24. (Rejected) The system of claim 22, wherein after said transfer, a second transfer of said digital asset can occur from either said first computer and/or said second computer, said second transfer further using a third instantiation of said digital asset and a third unique identifier.
25. (Rejected) The system of claim 22, wherein at least said second computer is a portable electronics device, including a personal computer, a personal digital assistant, and/or a telephone.
26. (Rejected) The system of claim 22, wherein said digital content includes an MP3 based audio file.

27. (Rejected) The system of claim 22, wherein said second unique identifier is based on combining information from any one or more of the following: a first id for said first computer, a second id for said second computer, an asset id for said digital asset, a customer id, a randomly generated number and/or a time of said transfer.
28. (Rejected) The system of claim 22, wherein a catalog of available digital assets is maintained at said first computer.
29. (Rejected) The system of claim 22, wherein said first software routine is also configured to execute an authorization routine, said authorization routine being adapted to secure agreement from a user of said second computer to access terms associated with said digital asset.
30. (Rejected) The system of claim 29, wherein said first routine is also configured to execute a setup routine, said setup routine being adapted to set up a transaction account with a digital asset management system separate from said first computer and said second computer, said transaction account including an identifier for a user of said second computer, identifiers for any transfers performed by said user, and billing information associated with said transfers.
31. (Rejected) The system of claim 29, wherein said first computer coordinates said transfer to said second computer in cooperation with a digital asset management system, such that said digital asset management system provides said second unique identifier.
32. (Rejected) The system of claim 31, wherein said first computer provides authorization for said digital asset management system to track all transfers of digital assets from said first computer.
33. (Rejected) The system of claim 32, wherein said first computer also performs hosting functions, and further receives credits from said digital asset management system for all authorized transfers made of digital assets.
34. (Rejected) The system of claim 29, wherein said second computer polls other computers coupled to the network to determine an optimal transfer source for said digital asset.
35. (Rejected) The system of claim 29, wherein said digital content includes content for a newspaper, a book, a magazine, and/or a periodical.

36. (Rejected) The system of claim 29, wherein said second instantiation of said digital asset is created in accordance with distribution rules in place at the time of said transfer, which distribution rules can be different from distribution rules in place at the time of creation of said first instantiation of said digital asset.
37. (Rejected) The system of claim 29, wherein said second computer is integrated within a fixed personal entertainment system, including a gambling machine, a digital jukebox, and/or a passenger seat.

38. (Withdrawn) A system for managing transfers of digital assets over a network, comprising:

- (a) a management computer coupled to the network; and
- (b) a first software routine executing on said management computer, said first software routine being adapted to prepare a digital asset for transfer over the network in accordance with a set of distribution rules;

wherein a modified version of said digital asset is generated by said first software routine, said modified version including a unique identification number associated with a first instantiation of said modified version of said digital asset; and

- (c) a second software routine executing on said management computer, said second software routine being adapted to track transfers of said digital asset over the network; and

wherein a separate instantiation of said digital asset is created for each transfer occurring over the network.

39. (Withdrawn) The system of claim 38, wherein said set of distribution rules are provided by a rights-holder management system, and include restrictions on terms of use and time periods of use.

40. (Withdrawn) The system of claim 39, wherein said set of distribution rules include information on title, author, and identification numbers for said digital asset.

41. (Withdrawn) The system of claim 38, wherein said unique identification number is embedded into said first instantiation of said modified version of said digital asset using a steganographic process.

42. (Withdrawn) The system of claim 38, wherein said transfers of said digital asset take place in a peer-to-peer manner over the network in coordination with said management computer and such that a complete tracking history for said digital asset is maintained by the system.

43. (Withdrawn) The system of claim 42, wherein said second software routine interfaces with a first client system and a second client system connected to the network in a peer to peer relationship, and provides unique identification numbers for each transfer occurring over the network between said first client system and said second client system.

44. (Withdrawn) The system of claim 38, wherein said first software routine further identifies network accessible locations available for transfers of said digital asset.
45. (Withdrawn) The system of claim 38, further including an accounting routine for performing accounting functions in connection with said transfers, including crediting of rights holders accounts, crediting of transaction host accounts, and/or debiting of user accounts.
46. (Withdrawn) The system of claim 38, further including a monitoring routine for performing authentication operations on digital assets stored and/or transferred between client systems over the network, said authentication operations including a determination of an embedded serial number of a digital asset and an identification of a last authorized transfer of said digital asset.
47. (Withdrawn) The system of claim 46, wherein adjustments to a user account, including access privileges, are made in accordance with the determinations made by said monitoring routine.
48. (Withdrawn) The system of claim 38, wherein a subsequent unique identification number used for a second instantiation of said digital asset is derived in part from said unique identification number.
49. (Withdrawn) The system of claim 48, wherein a tracking history for said digital asset, including all transfers over the network, can be derived from said subsequent unique identification number.
50. (Withdrawn) The system of claim 38, wherein at least some portions of said modified version of said digital asset are encrypted and/or contain steganographically processed data.
51. (Withdrawn) The system of claim 38, wherein distributions of said digital asset over said network are not preconditioned on securing authorization for individual copies of said digital asset.
52. (Withdrawn) The system of claim 38, wherein electronic indexes and catalogs are provided by the management computer for facilitating locating and transferring of said digital asset.

53. (Withdrawn) A method of distributing digital assets in a peer-to-peer connectable environment across a network, including between a first peer network device and a second peer network device, the method comprising the steps of:

- (a) introducing a digital asset into the peer-to-peer connectable environment, said digital asset having an associated first set of distribution rules; and
- (b) storing and distributing said digital asset at a first network accessible location so that a transfer of said digital asset can be made by the first peer network device and/or the second peer network device; and
- (c) generating a tracking record associated with said transfer; and
- (d) repeating at least step (c) for any subsequent transfers of said digital asset within the network;

wherein said transfer as well as any of said subsequent transfers over the network involving said digital asset between the first peer network device, the second peer network device and/or the first network accessible location are processed in accordance with said first set of distribution rules and are associated with tracking records.

54. (Withdrawn) A method of introducing digital assets into an electronic network distribution system, comprising the steps of:
- (a) receiving and storing a digital asset on a first computer coupled to the electronic network distribution system; and
 - (b) processing administration information for said digital asset, including an asset identifier and a rights-holder identifier;
 - (c) associating said administration information with said digital asset; and
 - (d) interacting with a digital asset management system to generate a modified version of said digital asset, said modified version of said digital asset being based on said administration information and tracking history information provided by said digital asset management system;
 - (e) posting said modified version of said digital asset to a location suitable for download by client devices from the electronic network distribution system;
- wherein said modified version of said digital asset is configured so that a tracking history can be maintained by said digital asset management system of each transfer of separate instantiations of said digital asset between peer devices coupled to the electronic network distribution.

55. (Rejected) A method of exchanging digital assets over a network, comprising the steps of:

(a) storing a digital asset on a first computer coupled to the network, which digital asset includes both digital content and a first unique identifier associated with a first instantiation of said digital asset; and

(b) setting up a customer account with said first computer including an authorization to play said digital asset on a second computer coupled to said first computer over the network; and

(c) creating a second instantiation of said digital asset, including a second unique identifier;

wherein said second unique identifier includes customer information associated with a customer for said digital asset;

(d) storing said second instantiation of said digital asset at said second computer; wherein said digital asset has no copy protection and can be transferred from said second computer to a third computer by said customer without requiring an additional authorization from said first computer.

56. (Withdrawn) A method of managing transfers of digital assets over a network, comprising the steps of:

(a) coupling a digital asset management computer to the network; and

(b) providing a digital asset to said digital asset management computer; and

(c) providing a set of distribution rules for said digital asset; and

(d) preparing a modified version of said digital asset for transfer over the network in accordance with said set of distribution rules, said modified version including a unique identification number associated with a first instantiation of said modified version of said digital asset; and

(e) tracking transfers of said digital asset over the network;

wherein a separate instantiation of said digital asset is created for each transfer occurring over the network.

57. (Withdrawn) A method of providing a digital asset for distribution comprising the steps of:

- (a) preparing a digital asset for distribution over an electronic network, said digital asset including digital content that is associated with a digital rights holder;
 - (b) providing a serial number for said digital asset, said serial number being uniquely identified with a first introduction of digital asset for distribution within said electronic network; and
 - (c) embedding said serial number within said digital asset so as to generate a first instantiation of said digital asset suitable for distribution over said electronic network; and
 - (d) placing said first instantiation of said digital asset in one or more locations accessible by users of said electronic network; and
 - (e) providing a list of said one or more locations so that said users of said electronic network can locate said first instantiation of said digital asset;
 - (f) updating a transaction database associated with said digital asset to reflect an occurrence of said first instantiation of said digital asset;
 - (g) updating a digital asset index database with administrative information associated with said digital asset, including a list of said one or more locations, terms of use of said digital asset and category information for said digital asset;
- wherein users of said electronic network can monitor said digital asset index database before electing to access said first instantiation and/or later instantiations of said digital asset.

58. (Withdrawn) A method of distributing a digital asset within an electronic network comprising the steps of:

(a) providing an index of digital assets available for distribution over the electronic network, each digital asset having a first serial number associated with a first transfer within the network, and including digital content that is associated with a digital rights holder;

wherein said index includes a list of one or more locations for said digital assets, terms of use of said digital assets and category information for said digital assets; and

(b) providing a second serial number for said digital asset in response to a request for a second transfer of a digital asset, said second serial number being embedded within said digital asset; and

(c) transferring said digital asset from a host server to a client device in response to a confirmation of acceptance of said terms of use for said digital asset; and

(d) updating a transaction database associated with said digital asset to reflect said second transfer of said digital asset.

60. (Rejected) The method of claim 55, further including a step: storing said second unique identifier as part of said digital asset.

61. (Rejected) The method of claim 55, further including a step transferring said digital asset between said first computer and said second computer in a peer to peer manner across the Internet.

62. (Rejected) The method of claim 55, further including a step: performing a second transfer of said digital asset from either said first computer and/or said second computer, said second transfer further using a third instantiation of said digital asset and a third unique identifier.

63. (Rejected) The method of claim 55, wherein at least said second computer is a portable electronics device, including a personal computer, a personal digital assistant, and/or a telephone.

64. (Rejected) The method of claim 55, wherein said digital content includes an audio file.

65. (Rejected) The method of claim 55, wherein said second unique identifier is based on combining information from any one or more of the following: a first id for said first computer, a second id for said second computer, an asset id for said digital asset, a customer id, a randomly generated number and/or a time of said transfer.
66. (Rejected) The method of claim 55, wherein a catalog of available digital assets is maintained at said first computer.
67. (Rejected) The method of claim 55, wherein said first software routine is also configured to execute an authorization routine, said authorization routine being adapted to secure agreement from a user of said second computer to access terms associated with said digital asset.
68. (Rejected) The method of claim 55, wherein said first routine is also configured to execute a setup routine, said setup routine being adapted to set up a transaction account with a digital asset management system separate from said first computer and said second computer, said transaction account including an identifier for a user of said second computer, identifiers for any transfers performed by said user, and billing information associated with said transfers.
69. (Rejected) The method of claim 55, wherein said first computer coordinates said transfer to said second computer in cooperation with a digital asset management system, such that said digital asset management system provides said second unique identifier.
70. (Rejected) The method of claim 68, wherein said first computer provides authorization for said digital asset management system to track all transfers of digital assets from said first computer.
71. (Rejected) The method of claim 68, wherein said first computer also performs hosting functions, and further receives credits from said digital asset management system for all authorized transfers made of digital assets.
72. (Rejected) The method of claim 55, wherein said second computer polls other computers coupled to the network to determine an optimal transfer source for said digital asset.
73. (Rejected) The method of claim 55, wherein said digital content includes content for a newspaper, a book, a magazine, and/or a periodical.

74. (Rejected) The method of claim 55, wherein said second instantiation of said digital asset is created in accordance with distribution rules in place at the time of said transfer, which distribution rules can be different from distribution rules in place at the time of creation of said first instantiation of said digital asset.
75. (Rejected) The method of claim 55, wherein said second computer is integrated within a fixed personal entertainment system, including a gambling machine, a digital jukebox, and/or a passenger seat.

76. (Rejected) A method of exchanging digital assets over a network, comprising the steps of:

- (a) providing a first computing system coupled to the network;
 - (b) storing a digital asset in one or more storage systems accessible to said first computing system, which digital asset includes both digital content and a first unique identifier associated with a first instantiation of said digital asset; and
 - (c) providing a second computing system which is coupled to the network and implements a digital asset management system which stores transaction information concerning said digital asset;
 - (d) selectively coupling said first computing system to a third computing system in response to a request made for said digital asset by a routine executing on behalf of said third computing system; and
 - (e) processing said request at said second computing system to generate an authorization for a transfer of said digital content of said digital asset;
 - (f) determining which one or more of said one or more storage systems should be used to transfer said digital content for said digital asset;
 - (g) creating a second instantiation of said digital asset for said request, including a second unique identifier; wherein said second unique identifier includes customer information associated with a customer for said digital asset;
 - (h) transferring said second instantiation of said digital asset, including said second unique identifier, to said third computing system from one or more of said one or more storage systems based on said authorization;
- updating said transaction information at said second computing system based on said transfer;

wherein each transfer of said digital asset between different computing systems is associated with a unique identifier embedded within the digital asset to facilitate tracking across the network, such that different versions of the digital asset are created for said transfers, and each version carries a complete transaction record of transfers of prior versions.

77. (Rejected) The method of claim 75, wherein said authorization includes a right to host said digital asset at said third computing system.
78. (Rejected) The method of claim 75 further including a step: crediting a rights holder account based on said transfer of said digital asset.
79. (Rejected) The method of claim 75 further including a step: debiting a customer account based on said transfer of said digital asset.
80. (Rejected) The method of claim 75, further including a step: determining whether one or more of said storage systems is storing an unauthorized version of said digital asset.
81. (Rejected) The method of claim 79, further including a step: determining a source of a prior transfer of said unauthorized version of said digital asset.
82. (Rejected) The method of claim 22 further including a step: recording a time stamp associated with each transfer of said digital asset across the network.
83. (Rejected) The method of claim 22 wherein said digital asset includes an associated advertisement.
84. (Rejected) The method of claim 22: further including a step: converting a second digital asset on said second computer to a second instantiation of said second digital asset including a third unique identifier including customer information associated with a customer for said second digital asset; further wherein said second digital asset has no copy protection and can be transferred from said second computer to a third computer by said customer without requiring an additional authorization from said first computer.